



Evaluation des systèmes électroniques programmables relatifs à la sécurité des installations industrielles dans le contexte des nouvelles normes

Philippe Villeneuve de Janti, Jean-Luc Durka

► To cite this version:

Philippe Villeneuve de Janti, Jean-Luc Durka. Evaluation des systèmes électroniques programmables relatifs à la sécurité des installations industrielles dans le contexte des nouvelles normes. Préventech, Mar 1995, Paris, France. ineris-00971918

HAL Id: ineris-00971918

<https://hal-ineris.archives-ouvertes.fr/ineris-00971918>

Submitted on 3 Apr 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



INSTITUT NATIONAL DE L'ENVIRONNEMENT INDUSTRIEL ET DES RISQUES

**Evaluation des systèmes électroniques programmables
relatifs à la sécurité des installations industrielles
dans le contexte des nouvelles normes**

Philippe VILLENEUVE de JANTI
Chef de Produits
Electronique - Sécurité des Systèmes
INERIS

Jean-Luc DURKA
Responsable du Laboratoire
de Sécurité des Systèmes Electroniques
INERIS



Evaluation des systèmes électroniques programmables relatifs à la sécurité des installations industrielles dans le contexte des nouvelles normes

I Introduction

Actuellement, les exploitants de process industriels se tournent vers des organismes indépendants pour faire valider les performances de leurs systèmes de gestion des fonctions de sécurité. Cette démarche, non-obligatoire, est cependant motivée par un souci d'obtenir un meilleur niveau de sécurité atteint par leurs systèmes.

Il n'y a pas de référentiels bien établis sur lesquels s'appuyer. Cependant, des projets de norme sont en cours d'élaboration, notamment aux niveaux allemand, européen et international, à savoir :

- Measurement and control - Fundamental safety aspects for measuring and control protective equipment, DIN V 19250 et DIN V 0801.
- Safety of Machinery ; Safety related parts of control systems ; Part 1 : General principles for design, Part 2 : Validation, Pr EN 954-1 et EN 954-2.
- Draft IEC 1508 : Functional safety : safety-related systems,

Pour déterminer les exigences de sécurité, il est nécessaire de définir la classe d'exigence, en fonction du domaine d'utilisation et des risques encourus.

Pour être pragmatique, nous allons considérer un process industriel de la chimie ou de la pétrochimie, et effectuer une analyse des risques au regard des trois référentiels précités.

Nous formulons donc les hypothèses suivantes :

- En cas d'incident, la protection du process est réalisée par le système de gestion des sécurités. L'événement indésirable est le masquage d'une ou de plusieurs fonctions de sécurité dont les conséquences peuvent être la destruction de l'installation et des pertes humaines.
- Si des personnes sont présentes dans la zone dangereuse, la mort de plusieurs personnes peut être considérée.
- Il est considéré que le séjour dans la zone dangereuse de plusieurs personnes est relativement rare.
- En l'absence du système de gestion des sécurités, la probabilité d'occurrence d'une situation dangereuse est relativement élevée.

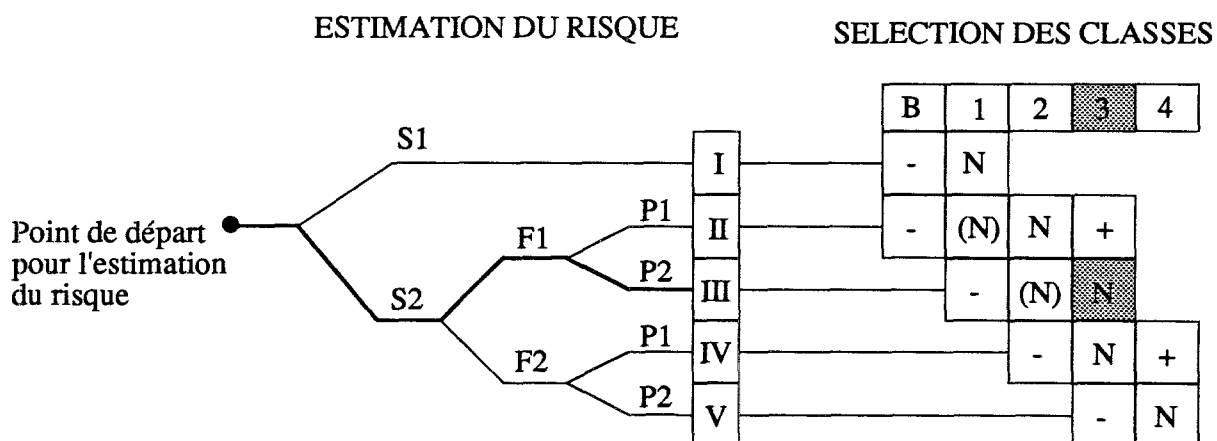


II Classification du risque selon le projet de norme EN 954-1

Compte tenu des hypothèses précédentes, nous attribuons aux paramètres les valeurs suivantes :

- 1. Gravité des lésions : -> S2
- 2. Fréquence et durée d'exposition : -> F1
- 3. Possibilité d'éviter le phénomène dangereux : -> P2

En effet, lorsqu'un phénomène dangereux se produit, il n'y a pratiquement aucune chance de l'éviter compte tenu de sa vitesse d'évolution.



Graphe des risques et classes d'exigence

Cette analyse des risques selon le projet de norme européen s'applique, en fait, à la sécurité des machines, et plus particulièrement, aux parties du système de commande relatives à la sécurité. A titre informatif, et compte tenu de l'état d'avancement des travaux sur ce sujet, nous pouvons néanmoins en déduire des exigences techniques, applicables au système de sécurité, pour une classe d'exigence de **niveau 3**.

Nous pouvons maintenant définir les exigences techniques pour un système dédié à la sécurité de classe d'exigence 3 selon le projet de norme EN 954-1.

Les parties du système de commande relatives à la sécurité doivent au minimum être conçues, élaborées, sélectionnées, montées et combinées, en accord avec les normes européennes relatives au domaine d'application concernant les principes de sécurité de base, de façon à ce qu'elles puissent faire face :

- aux contraintes de fonctionnement prévues,
- aux autres influences extérieures.



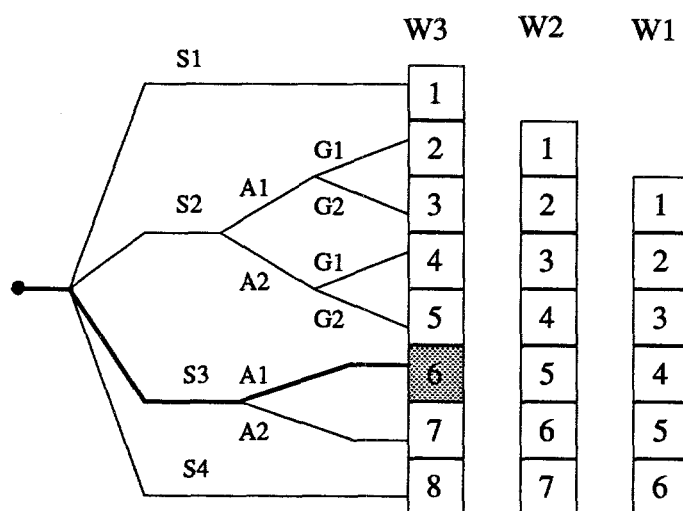
De plus, elles doivent être conçues et élaborées en utilisant des principes et des composants éprouvés. Enfin, le système de gestion des sécurités doit être conçu pour qu'un défaut unique de la commande n'entraîne pas la perte d'une des fonctions de sécurité. "Certains défauts" (sic) doivent être détectés par des mesures adaptées. Le système de sécurité génère alors un signal de sortie conduisant à un état sûr.

Après détection d'un défaut, l'état sûr doit être maintenu tant que le problème n'est pas réglé. L'accumulation de défauts non détectés pouvant conduire à la perte de la fonction de sécurité correspond donc à l'événement redouté.

III Classification du risque selon le projet de norme DIN V 19250

Compte tenu des hypothèses précédentes, nous attribuons aux paramètres les valeurs suivantes :

1. Gravité des lésions : -> S3
2. Fréquence et durée d'exposition : -> A1
3. Probabilité d'occurrence de l'événement indésirable : -> W3



Graphe des risques et classes d'exigence

Cette analyse des risques selon le projet de norme allemand s'applique, tout à fait, au système de sécurité du process. Nous déterminons donc une classe d'exigence de niveau 6. Cependant, il est généralement admis une classe d'exigence de **niveau 5** pour les process chimiques, compte tenu de la très faible fréquence d'accident.



En effet, pour que l'événement redouté se produise, la conjonction de quatre événements doit être réalisée :

- réaction dangereuse au niveau du process,
- défaillance du système de contrôle commande,
- défaillance du système de gestion des sécurités,
- et défaillance des sécurités ultimes.

Nous pouvons maintenant définir les exigences techniques pour un système dédié à la sécurité de classe d'exigence 5 selon le projet de norme DIN V VDE 0801.

Le tableau, ci-après, décrit pour les mesures d'évitement et les mesures de contrôle des défauts leur efficacité, en fonction de la nature et des causes de ces défauts pour la classe d'exigence 5.

Mesures de sécurité particulières	Efficacité
1. Contrôler les défauts aléatoires uniques dans le matériel	mesures renforcées (élevée)
2. Contrôler les défauts aléatoires multiples dans le matériel, encourus par une accumulation de défauts	mesures simples (moyenne)
3. Eviter les défauts systématiques dans le matériel	mesures courantes (basse)
4. Contrôler les défauts systématiques dans le matériel	aucune mesure
5. Eviter les défauts systématiques dans le logiciel	mesures simples (moyenne)
6. Contrôler les défauts systématiques dans le logiciel	mesures courantes (basse)
7. Eviter les erreurs de manoeuvre, de mise en marche et de manipulation	mesures simples (moyenne)
8. Eviter les erreurs dus à des influences opérationnelles et d'environnement	mesures simples (moyenne)
9. Contrôler les erreurs dus à des influences opérationnelles et d'environnement	mesures courantes (basse)

En conséquence, le système de sécurité doit être conçu en respectant notamment les mesures suivantes :

- Architecture à deux voies avec comparaison de résultats ou d'états du système.
- Tests complémentaires.
- Matériel éprouvé en service et composants homologués.

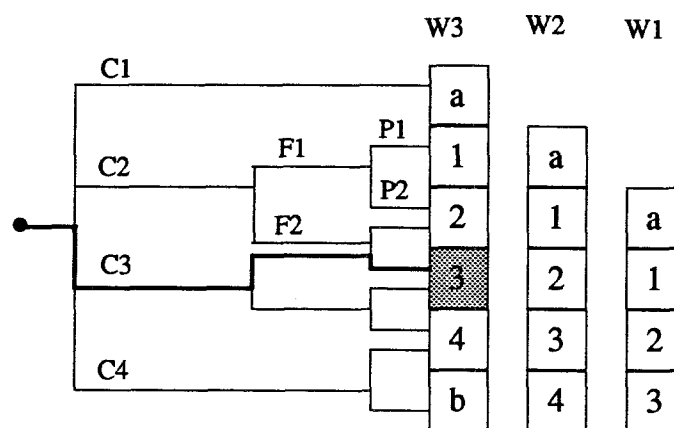


- Contrôle des mesures et propriétés requises, notamment par simulation de défauts.
- Vérification du codage.
- Contrôle de toutes les branches, de tous les modules logiciels.
- Contrôle de toutes les conditions temporelles et interruptions.
- Contrôle fonctionnel complémentaire du système complet.

IV Classification du risque selon le projet de norme IEC 1508

Compte tenu des hypothèses précédentes, nous attribuons aux paramètres les valeurs suivantes :

- 1. Gravité des lésions : -> C3
- 2. Fréquence et durée d'exposition : -> F1
- 2. Possibilité d'éviter le danger : -> P2
- 3. Probabilité d'occurrence de l'événement indésirable : -> W3



Le domaine d'application de ce projet de norme concerne les systèmes de sécurité utilisés dans :

- les process industriels (arrêt d'urgence, détection de gaz),
- les industries manufacturières (robots,),
- le transport (signalisation ferroviaire, ascenseur),
- le médical.

En ne considérant que l'approche probabiliste de l'IEC 1508, l'intégrité du système concerne deux éléments :

- L'intégrité du système "matériel" : le niveau d'intégrité du système "matériel" peut être normalement estimé pour les défauts aléatoires uniques. Le tableau ci-dessous présente les valeurs des taux de défaillance dangereuse pour les niveaux d'intégrité du système.

Niveau d'intégrité du système	Fonctionnement continu de la fonction de sécurité (probabilité de défaillance dangereuse par heures)	Fonctionnement sur demande de la fonction de sécurité (probabilité de défaillance de la fonction sur demande)
4	$10^{-8} < \lambda_d < 10^{-9}$	$10^{-4} < \lambda_d < 10^{-5}$
3	$10^{-7} < \lambda_d < 10^{-8}$	$10^{-3} < \lambda_d < 10^{-4}$
2	$10^{-6} < \lambda_d < 10^{-7}$	$10^{-2} < \lambda_d < 10^{-3}$
1	$10^{-5} < \lambda_d < 10^{-6}$	$10^{-1} < \lambda_d < 10^{-2}$

Niveau d'intégrité du système : objectif des taux de défaillance

- L'intégrité du système "systématique" : les défauts systématiques sont relatifs aux erreurs de conception, aux erreurs logicielles, aux défaillances de mode commun, etc.. Pour réduire ces défauts, des procédures techniques, des mesures, sont recommandées.

V Synthèse sur la normalisation

La classification des risques, telle qu'elle est définie dans le projet de norme EN 954-1, ne s'applique, en fait, que pour les machines dangereuses (elle est associée à la Directive Machines). C'est le constat que nous faisons à l'issue de cette étude. Le projet de norme international, quant à lui, s'inscrit dans une approche système et intègre une approche également probabiliste.

Par ailleurs, dans le projet de norme EN 954-1, les principes généraux exposés laissent envisager un certain nombre de problèmes, quant à la mise en oeuvre, et plus particulièrement, pour la validation des composants électroniques complexes dont l'emploi se généralise avec la rapidité que l'on sait.

La correspondance entre niveaux de risque n'est pas réellement possible car les approches ne sont pas identiques. Dans l'IEC 1508 par exemple, l'approche probabiliste est retenue. De plus, on s'intéresse à des champs d'application et à des niveaux de gravité différents. Les spécialistes s'accordent à l'heure actuelle sur la correspondance suivante :

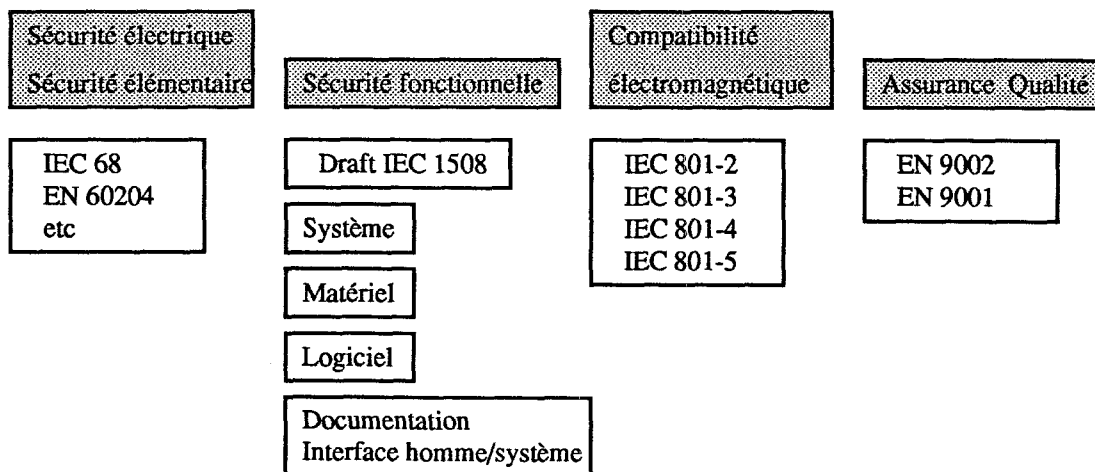
DIN V 19250	Draft IEC 1508
1	0
2-3	1
4	2
5-6	3
7-8	4

Nous pouvons noter qu'il existe actuellement des divergences, entre spécialistes, sur cette correspondance entre le projet de norme européen et les autres projets. Cela est principalement dû au fait que les échelles de gravité des dangers ne se recouvrent pas. De plus, dans le cadre de la Directive Machines, la notion de niveau tolérable de risque ne fait pas l'objet d'un consensus.

VI La démarche de l'INERIS

La présente procédure a pour objet de définir le référentiel d'évaluation d'un système de gestion de fonctions de sécurité. Les spécifications techniques ont été élaborées d'une part, à partir de notre propre expérience, et d'autre part, en harmonie avec la normalisation allemande, européenne et internationale.

Elle se décompose en quatre phases principales :





La première phase, représentant 20 % du travail de l'évaluation du système, a pour objet de valider, d'une part, les aspects liés à la sécurité électrique, et d'autre part, son bon fonctionnement vis-à-vis des contraintes d'environnement auxquelles ce dernier est susceptible d'être confronté.

Les essais de type normatifs concernent plusieurs catégories :

- climatiques : essais de robustesse au froid et à la chaleur sèche, variation de température, essais de robustesse au cycle de chaleur humide ;
- mécaniques : vibrations et chocs ;
- électriques : ondes oscillatoires amorties, essais de variation de fréquence et de la tension du réseau d'alimentation, immunité au troisième harmonique, interruptions de tension d'alimentation ;
- relatifs à la sécurité : Exigences vis-à-vis des chocs électriques, essais de rigidité diélectrique, essais de continuité de la terre de protection, etc.

La seconde phase, représentant 50 % du travail de l'évaluation, se décompose en quatre étapes :

1. l'analyse structurale au niveau du système :

- * vérification de la structure fonctionnelle.
- * analyse des modes communs.

2. l'évaluation de la structure Matérielle, cette étape intègre :

- * une analyse des modes de défaillances et de leurs effets réalisée au niveau fonctionnel pour l'ensemble du système, puis au niveau composant pour les points critiques liés à la sécurité,
- * l'analyse des solutions de traitement des risques résiduels (configuration, chien de garde, RAM, ROM, E/S, ...),
- * l'analyse du comportement sur défaut interne (injections physiques de défaillances sur le système pour les points critiques dont le comportement n'a pas pu être validé par analyse).

3. l'évaluation de la structure Logiciel : celle-ci est menée selon les axes suivants:

- * analyse du dossier documentaire, du point de vue de sa constitution, de l'image qu'il donne du cycle de développement,
- * analyse structurale du programme quant à la spécification correcte et complète des fonctions de sécurité fixées dans la phase de concept,
- * analyse de la structure globale du logiciel pour chaque fonction élémentaire,
- * analyse exhaustive des procédures d'autocontrôle,

- * analyse de l'efficacité et du recouvrement des autocontrôles ainsi que le temps de cycle des autocontrôles,
- * analyse des documents relatifs aux tests par simulation d'erreurs de logiciel.

4. l'analyse des règles de mise en oeuvre dont le but est de limiter les erreurs de l'opérateur, par une bonne prise en compte de ses interventions lors de la conception :

- * qualité des documentations,
- * qualité des techniques d'aide à la maintenance,
- * qualité des signalisations.

La troisième phase, représentant 20 % du travail de l'évaluation, a pour but de valider la robustesse du système vis-à-vis des perturbations d'origine électromagnétique. Les essais suivants sont réalisés :

- * décharges électrostatiques,
- * champs électromagnétiques rayonnés,
- * transitoires électriques rapides en salves,
- * fortes énergies.

Enfin la dernière phase, représentant 5 à 10 % du travail de l'évaluation, porte sur la gestion et l'assurance de la qualité que le constructeur doit mettre en oeuvre pour assurer le maintien de la conformité de son système aux caractéristiques évaluées.

VII Conclusion

L'INERIS joue un rôle actif dans les travaux des comités de normalisation internationale, portant sur les dispositifs et systèmes électroniques programmables ou complexes, et utilisés pour assurer la sécurité des machines et des installations. Il est ainsi possible d'apporter des conseils et des réponses aux questions des exploitants aussi bien que des constructeurs d'équipements. Des procédures de validation du niveau d'intégrité de ces systèmes ont été élaborées et s'appuient sur ces travaux en y intégrant leur orientation prévisible.

En europe, le projet EN 954-1 donne lieu à des interprétations divergentes par les organismes de sécurité. C'est pourquoi, l'INERIS en étroite collaboration avec l'INRS, coordonne actuellement une action pour lancer un projet européen dont l'objet sera d'accélérer l'émergence de la norme EN 954, et tout particulièrement, pour harmoniser les procédures de validation des laboratoires européens.